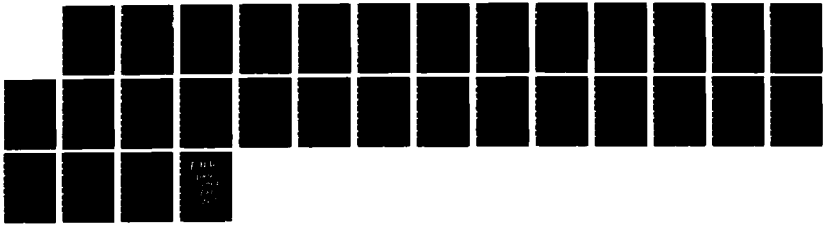
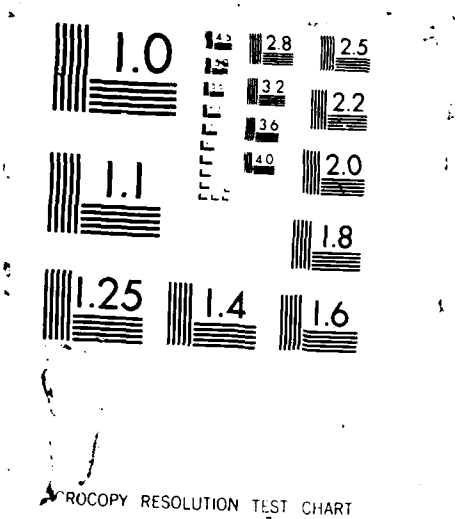
AD-A186 311 INADEQUACY OF CONVENTIONAL DYNAMIC RECOVERY MECHANISMS 1/1
IN THE PRESENCE OF (U) STANFORD UNIV CA CENTER FOR
RELIABLE COMPUTING H H AMER ET AL JUN 87 CRC-TR-87-11
UNCLASSIFIED N00014-85-K-0600 F/G 12/6 NL




1.0
1.1
1.25
1.4
1.6
1.8
2.0
2.2
2.5
2.8
3.2
3.6
4.0
ROCOPY RESOLUTION TEST CHART

SEC[illegible]

# AD-A186 311

MENTATION PAGE

DTIC FILE COPY

| | |
|---|---|
| 1a REPORT SECURI UNCLASSIFI | 1b RESTRICTIVE MARKINGS NA |
| 2a SECURITY CLAS[illegible] NA | 3 DISTRIBUTION / AVAILABILITY OF REPORT Approved for public release; distribution unlimited |
| 2b DECLASSIFICATION / DOWNGRADING SCHEDULE NA | |
| 4 PERFORMING ORGANIZATION REPORT NUMBER(S) CRC 87-11 (CSL-TN-87-329) | 5 MONITORING ORGANIZATION REPORT NUMBER(S) N00014-85-K-0600 |
| 6a NAME OF PERFORMING ORGANIZATION Center for Reliable Computing | 6b OFFICE SYMBOL (If applicable) |
| 7a NAME OF MONITORING ORGANIZATION Resident Representative, ONR | |
| 6c ADDRESS (City, State, and ZIP Code) ERL 460 Stanford University Stanford, CA 94305-4055 | 7b ADDRESS (City, State, and ZIP Code) Durand 165 Stanford University Stanford, CA 94305-2192 |
| 8a NAME OF FUNDING / SPONSORING ORGANIZATION ONR | 8b OFFICE SYMBOL (If applicable) |
| 9 PROCUREMENT INSTRUMENT IDENTIFICATION NUMBER 2 DPN540 | |
| 8c ADDRESS (City, State, and ZIP Code) Detachment, Pasadena 1030 E. Green St. Pasadena, CA 91106-2485 | 10 SOURCE OF FUNDING NUMBERS |

| PROGRAM ELEMENT NO | PROJECT NO | TASK NO | WORK UNIT ACCESSION NO |
|---|---|---|---|
| | | | |

DTIC ELECTE OCT 14 1987 S E

11 TITLE (Include Security Classification)
Inadequacy of Conventional Dynamic Recovery Mechanisms in the Presence of Temp. Failures

12 PERSONAL AUTHOR(S)
Hassanein H. Amer, Mario L. Cortes and Edward J. McCluskey

| 13a TYPE OF REPORT | 13b TIME COVERED | 14 DATE OF REPORT (Year, Month, Day) | 15 PAGE COUNT |
|---|---|---|---|
| technical report | FROM _____ TO _____ | June 1987 | 25 |

16 SUPPLEMENTARY NOTATION

| 17 COSATI CODES | | | 18 SUBJECT TERMS (Continue on reverse if necessary and identify by block number) |
|---|---|---|---|
| FIELD | GROUP | SUB-GROUP | |
| | | | |
| | | | |

19 ABSTRACT (Continue on reverse if necessary and identify by block number)

This paper shows that some implementations of fault-tolerant systems with dynamic error detection and reconfiguration mechanisms may not recover from certain types of temporary failures. An experiment is conducted to study the effect of temporary failures on the behavior of a dynamically redundant fault-tolerant system. The system is built out of LSTTL catalog parts. Transient failures are induced by reducing the power supply voltage; intermittent failures are induced by loading nodes in the system. Reducing the power supply voltage produces common-mode failures that can be detected if the recovery mechanism produces high amplitude oscillations when its inputs are near the threshold level. Intermittent failures can be detected if the recovery mechanism detects errors before incorrect data is transmitted through the output devices. It is shown that the stuck-at fault model is inappropriate for the temporary failures injected into the system. Techniques are suggested that will guarantee detection of many transient and intermittent failures.

| 20 DISTRIBUTION / AVAILABILITY OF ABSTRACT | 21 ABSTRACT SECURITY CLASSIFICATION |
|---|---|
| ☒ UNCLASSIFIED/UNLIMITED ☐ SAME AS RPT ☐ DTIC USERS | |
| 22a NAME OF RESPONSIBLE INDIVIDUAL E.J. McCluskey | 22b TELEPHONE (Include Area Code) 415/723-1451 / 22c OFFICE SYMBOL |

DD FORM 1473, 84 MAR — 83 APR edition may be used until exhausted. All other editions are obsolete.

SECURITY CLASSIFICATION OF THIS PAGE

Center for Reliable Computing





# INADEQUACY OF CONVENTIONAL DYNAMIC RECOVERY MECHANISMS IN THE PRESENCE OF TEMPORARY FAILURES

**Hassanein H. Amer, Mario L. Cȏrtes and Edward J. McCluskey**

CRC Technical Report No. 87-11
(CSL TN No. 87-329)

June 1987

**CENTER FOR RELIABLE COMPUTING**
Computer Systems Laboratory
Departments of Electrical Engineering and Computer Science
Stanford University
Stanford, California 94305 U.S.A.

Imprimatur: Henk Goosen and Takashi Nanya

This work was supported in part by the Innovative Science and Technology Office of the Strategic Defense Initiative Organization and administred through the Office of Naval Research under contract No. N00014-85-K-0600 and by the Egyptian Government.

# INADEQUACY OF CONVENTIONAL DYNAMIC RECOVERY MECHANISMS IN THE PRESENCE OF TEMPORARY FAILURES

Hassanein H. Amer, Mario L. Cortes and Edward J. McCluskey

CRC Technical Report No. 87-11
(CSL TN No. 86-329)

June 1987

**CENTER FOR RELIABLE COMPUTING**
Computer Systems Laboratory
Departments of Electrical Engineering and Computer Science
Stanford University
Stanford, California 94305 U.S.A.

## ABSTRACT

This paper shows that some implementations of fault-tolerant systems with dynamic error detection and reconfiguration mechanisms may not recover from certain types of temporary failures. An experiment is conducted to study the effect of temporary failures on the behavior of a dynamically redundant fault-tolerant system. The system is built out of LSTTL catalog parts. Transient failures are induced by reducing the power supply voltage; intermittent failures are induced by loading nodes in the system. Reducing the power supply voltage produces common-mode failures that can be detected if the recovery mechanism produces high amplitude oscillations when its inputs are near the threshold level. Intermittent failures can be detected if the recovery mechanism detects errors before incorrect data is transmitted through the output devices. It is shown that the stuck-at fault model is inappropriate for the temporary failures injected into the system. Techniques are suggested that will guarantee detection of many transient and intermittent failures.

**Keywords:** Fault-tolerant systems, Temporary failures, Dynamic recovery mechanisms.

TABLE OF CONTENTS

## LIST OF FIGURES



## LIST OF TABLES

# 1 INTRODUCTION

Fault-tolerant schemes often require hardware replication. A fault-tolerant system will recover from a fault if that fault does not simultaneously affect too many of the replicated modules. Consider a Triple Modular Redundant (TMR) system [Siewiorek 82]. It consists of three identical modules and a voter. The system will operate correctly if the voter and at least two of the three modules are fault-free. If a fault simultaneously affects two or more of the modules (common-mode failure), the system may produce erroneous outputs.

While the behavior of fault-tolerant systems in the presence of permanent failures is well established, the effect of temporary failures on these systems is not well understood. Temporary failures can be divided into transient and intermittent [Côrtes 86b] [McCluskey 86] [Siewiorek 82]. Transient failures are nonrecurring temporary failures caused by some externally induced signal perturbation usually due to radiation, power supply fluctuation, etc. Intermittent failures are recurring temporary failures caused by component degradation or poor design (violation of operating margins). The frequency of temporary failures is much higher than that of permanent failures. Experiments show that at least 80% of system failures are due to temporary failures [Iyer 82] [Siewiorek 82]. Therefore, it is very important to verify that fault-tolerant systems can recover from temporary failures.

[Côrtes 87] has a good survey about temporary failures. In this survey, it is mentioned that temporary failures are modeled as random

stuck-at faults. Temporary failures affecting memory cells can be modeled by the stuck-at fault model. Alpha particles can cause a cell to temporarily store an incorrect value. The effect of the failure will disappear when the information in the cell is overwritten. On the other hand, [Côrtes 86a] shows that, in some cases, temporary failures cannot be modeled by the stuck-at fault model. Therefore, it is important to verify that the stuck-at fault model can accurately explain the behavior of a fault-tolerant system with a temporary failure.

In this paper, a simple fault-tolerant system is described. The fault-tolerant technique used is dynamic redundancy [Lala 85] [Siewiorek 82]. A dynamically redundant system consists of several identical modules with only one of them operating at a time (the active module). The other modules serve as spares and replace the active module in case an error is detected in it. Dynamic redundancy requires concurrent (on-line) error detection and reconfiguration. The system under study is built out of LSTTL catalog parts (74LSxx series). It is then stressed using the methods described in [Côrtes 86b] to induce certain types of transient and intermittent failures. The output of the system is monitored in order to study the effectiveness of the error detection and reconfiguration circuitry in the presence of temporary failures. It is shown that, for this specific implementation of dynamic redundancy, some temporary failures are either not detected or the system is unable to reconfigure successfully. Furthermore, it is found that the stuck-at fault model is inappropriate for temporary failures and finally, techniques are suggested that will guarantee detection of many transient

## 2 SYSTEM DESCRIPTION

The function of the system under study is to perform the inclusive OR of its two inputs. The system uses dynamic redundancy for fault-tolerance [Losq 75]. Figure 1 shows the fault-tolerant system. It consists of two identical modules, X and Y, and a recovery mechanism. Module X is the active module and module Y is the powered spare. Module X (or Y) consists of two OR gates. The recovery mechanism consists of a detector and a switch. The detector is an XOR gate that compares the outputs of the two OR gates in module X. The switch consists of a J-K flip-flop and four buffers with tri-state outputs. Initially, the J-K flip-flop is reset (Q=0 and Q'=1) and the outputs of the OR gates in module X are connected to the system bus (bus-out1 and bus-out2). If the XOR gate detects a discrepancy between the outputs of the two OR gates in module X, its output goes to 1, the flip-flop output goes to 1 (Q=1), module X is disconnected from the bus and module Y is connected. A system failure occurs when incorrect data is transmitted over the system bus.

Figure 2 shows the system failure detector. This circuit compares the outputs of the fault-tolerant system (bus-out1 and bus-out2) to a reference output (ref-out). If the three signals disagree, the system failure signal (sys-fail) goes from 1 to 0 (active low).

Figure 3 shows the experimental setup. The lower box contains the actual fault-tolerant system. It has two 74LS32 (quadruple 2-input OR gates) chips, one for the active module and one for the spare module.

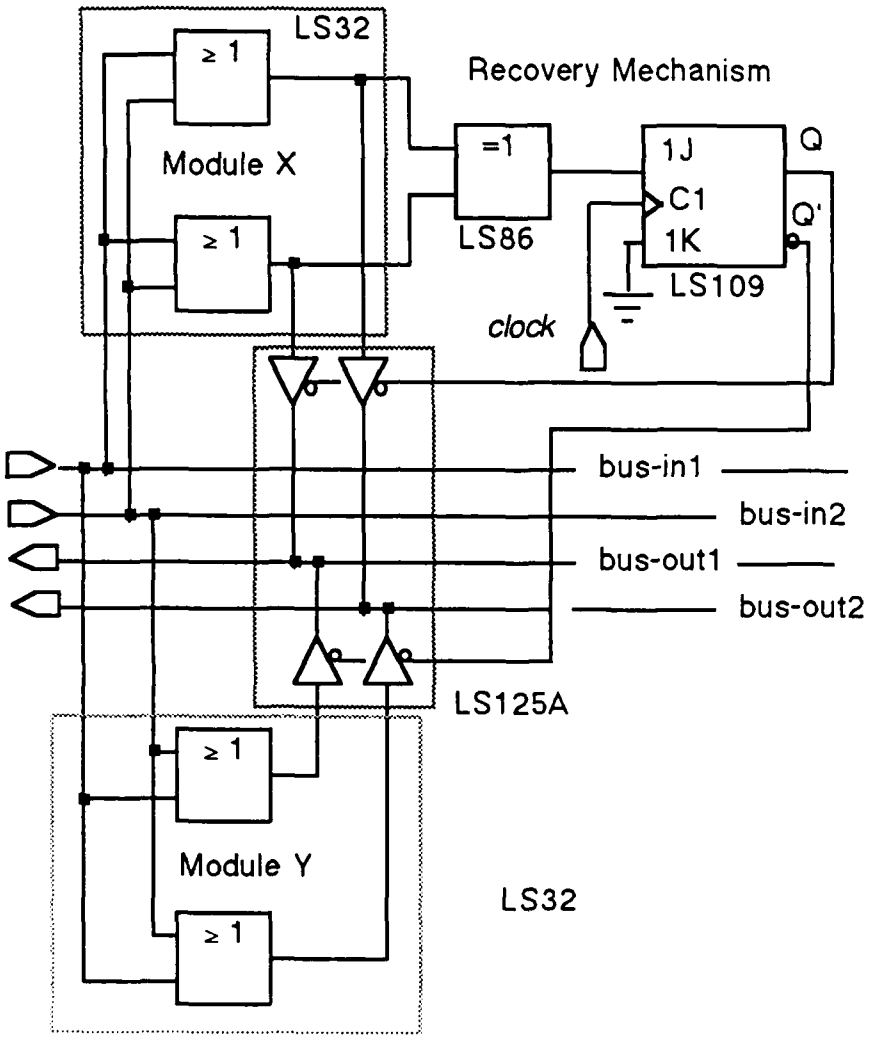



Fig. 1 Fault-Tolerant System

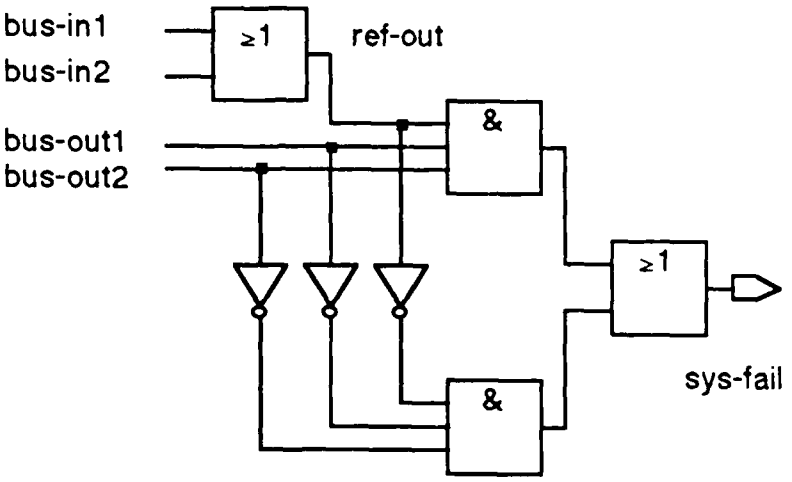



Fig. 2 System Failure Detector

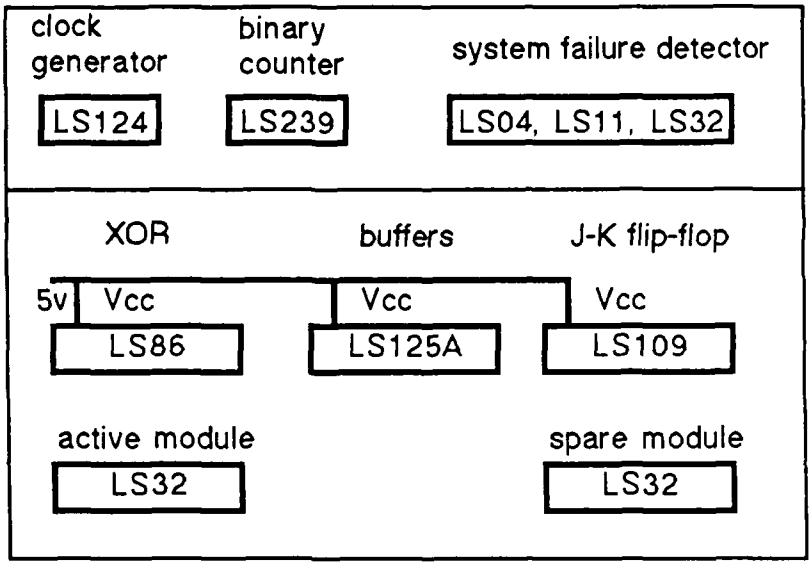



Fig. 3 Experimental Setup

The 74LS86 (quadruple 2-input XOR gates) is used as a detector and the 74LS109 as the switch (J-K flip-flop). A 74LS125A is used for buffering the system outputs. The upper box contains peripheral circuitry: a 74LS124 (dual votage-controlled oscillators) is used to generate the clock signal and a 74LS239 (4-bit binary counter) generates the inputs for the fault-tolerant system. A 74LS11 (triple 3-input AND gates) , a 74LS04 (hex inverters) and a 74LS32 are used to generate the reference output (ref-out) and compare it to the outputs from the system (bus-out1 and bus-out2). A system failure occurs when bus-out1 or bus-out2 are different from the reference output. A logic analyzer and an oscilloscope are used to monitor the behavior of the system.

# 3 INJECTION OF TEMPORARY FAILURES INTO THE SYSTEM

Experiments to evaluate the efficiency of recovery mechanisms in fault-tolerant systems have been reported in the literature. [Decouty 80] describes a tool to evaluate the efficiency of fault detection mechanisms. This tool generates permanent (s-a-0, s-a-1) faults, injects them into the system under study and observes the system behavior. [Crouzet 82] presents the results of an experiment using the tool described in [Decouty 80]; in this experiment stuck-at faults are injected into a microcomputer and its behavior is monitored. It is reported that approximately 99% of the injected faults are detected. In [Schuette 86], temporary s-a-0(1) faults are injected into a system to evaluate the coverage of the fault-tolerant schemes used in the system. In the papers mentioned above, temporary failures were modeled by the stuck-at fault model. [Côrtes 86b] shows that this model is not appropriate for intermittent failures. Therefore, more realistic fault injection methods need to be used.

In this experiment, the fault-tolerant system will be subjected to two types of stress: reduced supply voltage and load. The voltage stress simulates power supply disturbances that may cause transient failures by affecting the noise immunity. It is shown in [Côrtes 86a] that DC disturbances and pulsed disturbances have the same effect on chip behavior. Therefore, it is reasonable to limit the experiments described in this paper to DC disturbances. The loading stress reduces the drive capability and simulates leakage paths that could induce

intermittent failures [Côrtes 86b]. The system will be divided into three subsystems: 1) The active module 2) The spare module 3) The recovery mechanism. These three subsystems are in the lower box in Fig. 3.

Reducing the supply voltage of the active (or spare) module is accomplished by reducing the voltage connected to the Vcc pin of the 74LS32 containing the active (or spare) module. Reducing the voltage supply of the recovery mechanism is accomplished by tying the Vcc pins of the detector (XOR gate), switch (J-K flip-flop) and buffers to the same power supply and then reducing the voltage of that power supply.

Loading is accomplished by connecting a 1K ohm variable resistance between a node in the system and ground (or 5 volts). The resistance is then decreased until an error occurs. The effect of loading is such that the disturbed lead in not permanently stuck-at-0 or 1. To load the active (or spare) module, the variable resistance is connected between the output of one of the OR gates and ground (or 5 volts). To load the recovery mechanism, the variable resistance is connected between the output of the XOR gate and ground (or 5 volts).

# 4 SYSTEM BEHAVIOR WITH SUPPLY DISTURBANCES

## 4.1 Supply disturbances in the active module

The system is started with the active module connected to the system bus. The clock frequency is set at 5 KHz. At low frequency, errors caused by supply disturbances are due to noise immunity problems [Cortes 86a]. Figure 4 illustrates the DC noise margin. A gate is designed to produce an output voltage greater than or equal to $V_{OH(min)}$, the minimum high output voltage for worst-case output loading. Similarly, $V_{OL(max)}$ is the maximum low output voltage for worst-case output loading. For a logic 0 input, the corresponding voltage must be no more than $V_{IL(max)}$, the minimum low input voltage to guarantee the appropriate output logic level. For a logic 1 input, the corresponding voltage must be at least $V_{IH(min)}$. The difference between $V_{OH(min)}$ and $V_{IH(min)}$ is the high-level signal-line noise margin. Similarly, the low-level signal-line noise margin is the difference between $V_{IL(max)}$ and $V_{OL(max)}$.

The voltage is reduced at the Vcc pin of the 74LS32 containing the two OR gates of the active module. With an 74LS86 from Vendor A, a system failure is observed (via the system failure detector and the logic analyzer) and the recovery mechanism does not disconnect the active module from the bus. Figure 5 shows the waveforms observed on the oscilloscope as Vcc is decreased. When Vcc decreases, $V_{OH}$ decreases while $V_{OL}$ remains constant. The outputs of both OR gates in the active module behave similarly. When $V_{OH}$ reaches 1.85v, $V_{OL}$ increases

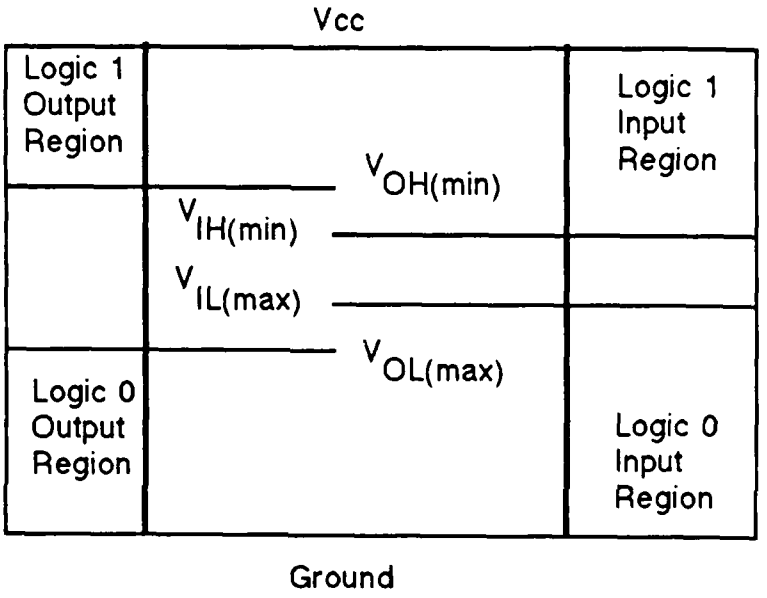



Fig. 4 DC Noise Margin

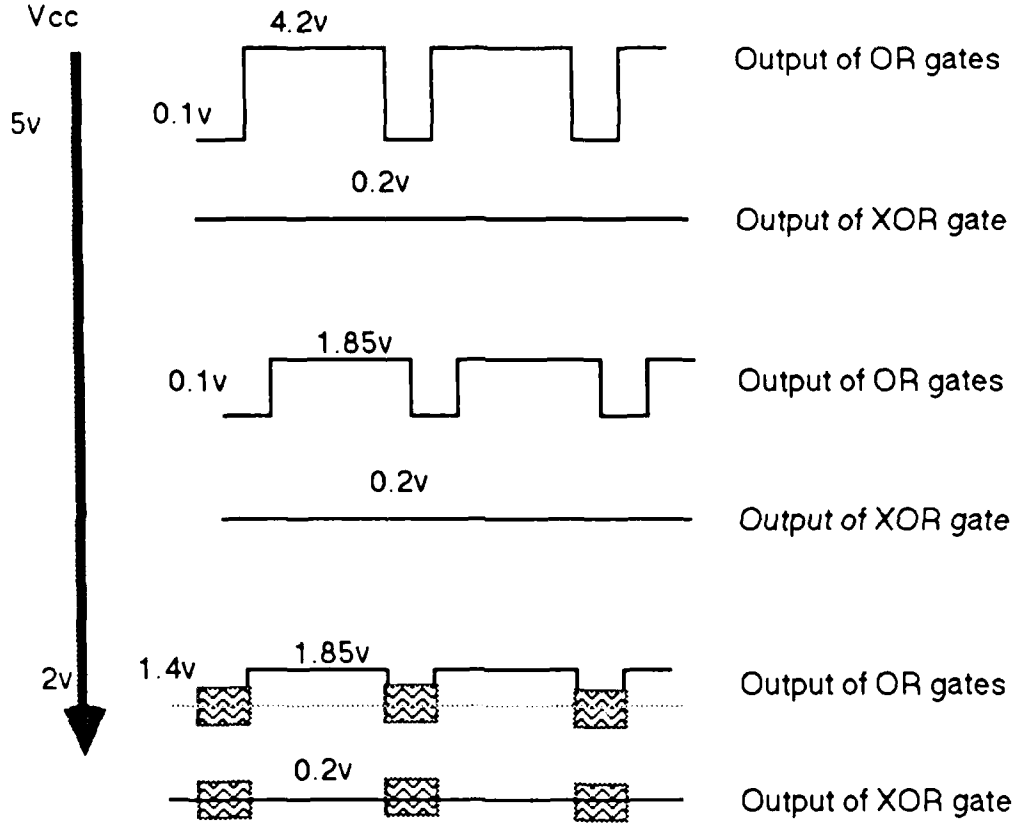



Fig. 5 System Behavior with XOR from Vendor A

gradually while $V_{OH}$ remains constant. At $V_{OL}$ = 1.4v, oscillations are observed when the output is low, and a system failure occurs. The buffer outputs are incorrect and the system failure detector (see Fig. 2) indicates a system failure because of the discrepancy between the signals on the bus and the reference output (ref-out in Fig. 2). The oscillations of $V_{OL}$ are interpreted by the buffer as a logic 1 while the correct output of the OR gates should be 0. During the entire experiment, the output of the XOR gate remained at 0.2v. Therefore, the detector was not able to detect the error and reconfigure the system by disconnecting the active module and connecting the spare.

The result of this experiment is intuitive. The power supply disturbance affected both OR gates in the active module thereby producing a common-mode failure that could not be detected. In other words, the stuck-at fault model could be used to describe the behavior of the system with power supply disturbances. The next experiment however, invalidates this theory.

The same experiment is repeated with an 74LS86 from vendor B. When Vcc for the active module (74LS32) is decreased, the system recovers successfully, i.e., the active module is disconnected from the bus and the spare module is connected. Figure 6 shows the waveforms observed on the oscilloscope. As in the previous experiment, $V_{OH}$ decreases when Vcc is decreased. Both OR gates in the active module behave similarly. When $V_{OH}$ reaches 1.85v, it remains constant and $V_{OL}$ starts increasing until it reaches 0.9v. At this point, the output of the XOR gate oscillates. The amplitude of the oscillations at the output of the XOR

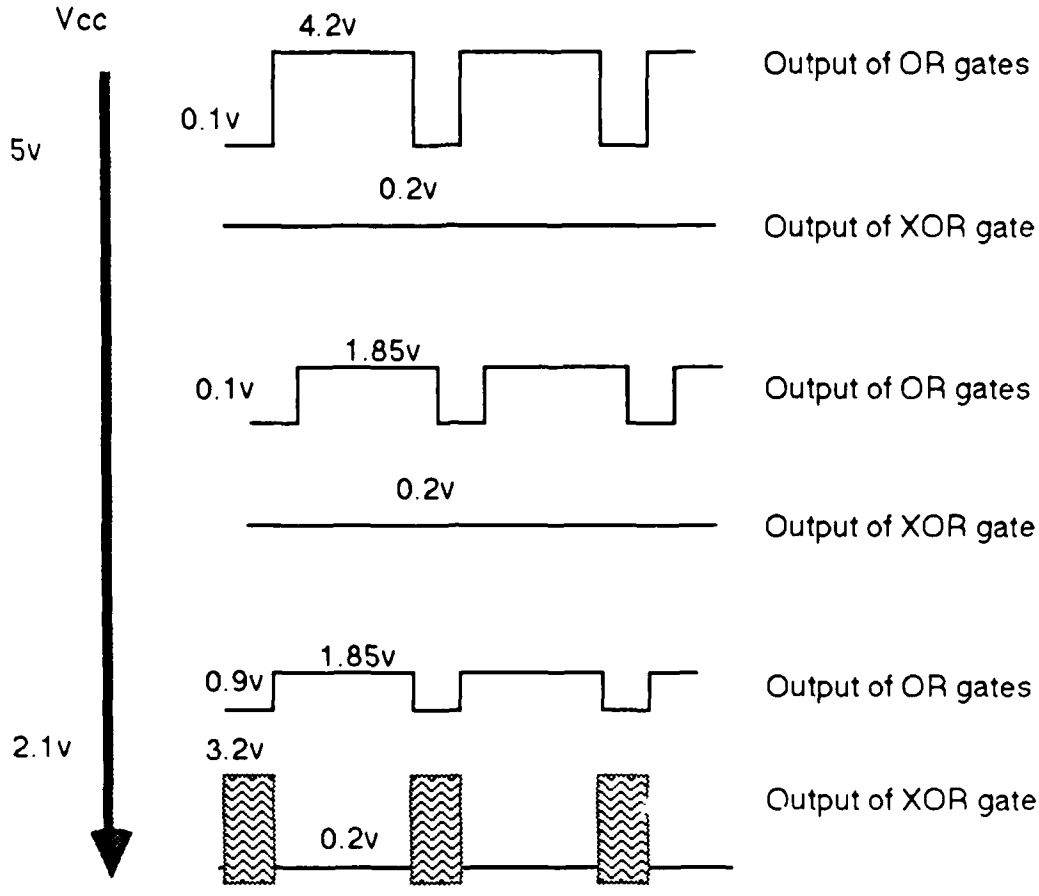



Fig. 6 System Behavior with XOR from Vendor B

gate is 3.2v. The J-K flip-flop interprets the oscillating signal at the output of the XOR gate as a logic 1, Q becomes 1 and the recovery is successful. The result of this experiment is counter-intuitive. The XOR gate detected the common-mode failure. Consequently, the stuck-at fault model cannot be used to represent transient failures due to power supply dips. The system will recover if the 74LS86 produces oscillations with an amplitude high enough to cause the J-K flip-flop to change states thereby disconnecting the active module from the bus and connecting the spare module. Depending on the electrical characteristics of the components used in the system, the oscillations at the output of the XOR gate could have occurred after incorrect data was transmitted over the bus thereby producing a system failure. Also, if the amplitude of the power supply dip were not high enough, the system would not have been affected at all. In summary, the possible outcomes of the experiment described above are:

No system failure (low amplitude power supply dip).

XOR with high amplitude oscillations:

Successful recovery before data corruption (Vendor B)

Data corruption before recovery

XOR with low amplitude oscillations:

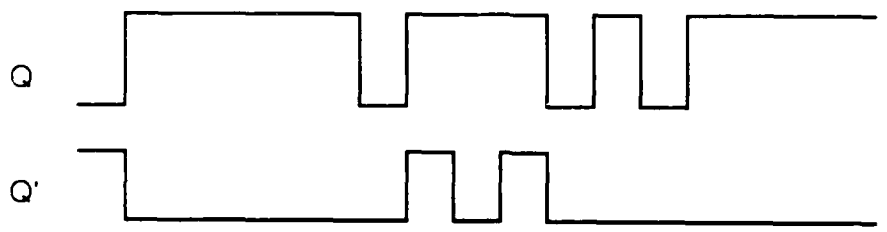
Data corruption and no recovery (Vendor A)

*Decreasing Vcc of the active module* is a good test to determine whether the XOR gate can detect a transient failure due to power supply fluctuation or not. The experiment reported in this section was repeated with XOR chips from two more vendors; in both cases, the XOR gates produced oscillations that caused the J-K flip-flop to change states and the system recovered successfully. In summary, XOR gates with high amplitude oscillations will be able to dectect the "common-mode" failure. The 74LS86 from vendor A produced oscillations of amplitude 0.2v. This amplitude was not high enough to cause the J-K flip-flop to change states.

A system using XORs from vendor A will be able to recover from transient failures due to power supply fluctuations if the two OR gates in the active module are on different chips. The experiment described above was repeated with an 74LS86 from vendor A and the two OR gates in the active module on different 74LS32s. Vcc of one of the 74LS32s was decreased and the system recovered successfully by disconnecting the active module from the bus and connecting the spare module.

## 4.2 Supply disturbances in the recovery mechanism

The Vcc pins of the chips containing the recovery mechanism (74LS86, 74LS109 and 74LS125A) are tied to the same power supply. With the active module connected to the system bus, Vcc for these three chips is lowered. Figure 7 shows the waveforms observed on the oscilloscope. A system failure occurs followed by a recovery (disconnection of active module and connection of the spare module). When the system failure




| | | |
|---|---|---|
| QQ'= | 01 | Active Connected to Bus |
| | 10 | *Spare Connected to Bus* |
| | 11 | Active and Spare Disconnected from Bus (System Failure) |

Fig. 7 Waveforms with Supply Disturbances in Recovery Mechanism

occurred, the Q and Q' outputs of the flip-flop were switching between 0 and 1. When Q and Q' were both 1, all four buffers were in the high impedance state, both modules (X and Y) were disconnected from the bus and the system had floating outputs and consequently failed because of data corruption. Eventually, Q settled at 1 and Q' at 0 but the recovery was too late.

In summary, the power supply dip caused the recovery mechanism to disconnect the active module from the bus and connect the spare. During the recovery, incorrect data was transmitted over the bus thereby producing a system failure.

# 5 SYSTEM BEHAVIOR WITH INTERMITTENT FAILURES

## 5.1 Intermittent failures in active module

A 1K ohm variable resistance is connected between the output of one of the OR gates in the active module and ground. With the active module connected to the system bus, the resistance is decreased until a system failure is observed. The loading stress reduces the drive capability and simulates leakage paths that could induce intermittent failures [Cortes 86a]. After the system failure, the J-K flip-flop changes state and the active module is disconnected from the system bus. The outputs of the two buffers were different before the XOR gate sensed the discrepancy and detected the error. The decreasing resistance pulls down the node it is connected to. The high output voltage ($V_{OH}$) at that node decreases. $V_{IL}$ for the buffers being higher than $V_{IL}$ for the XOR gate, the buffers go to 0 while the XOR gate still interprets the decreased voltage at the pulled down node, as a logic 1. $V_{IL}$ for the buffers and the XOR gate were determined experimentally. The buffer input was tied to a variable voltage source. Starting from 5 volts, the input voltage was decreased until the output of the buffer switched to the low output voltage. The input voltage at which the switching occured is $V_{IL}$. For the XOR gate, one of the inputs was connected to the variable voltage source while the other input was connected to : 1) logic 0, 2) logic 1. The logic 0 (logic 1) were obtained at the output of a buffer whose input was tied to ground (Vcc). Starting from 5 volts, the variable voltage was decreased until the output of the XOR

gate switched. The input voltage at which the switching occured is $V_{IL}$. The values of $V_{IL}$ and $V_{IH}$ specified by the manufacturer are 0.8v and 2v respectively. These values are more conservative than the ones determined experimentally to take into account variations in the manufacturing process. Table 1 shows the results of the experiment.

Table 1 $V_{IL}$ and $V_{IH}$ for the XOR gate and the buffers

| Experiment | $V_{IL}$ | $V_{IH}$ |
|---|---|---|
| XOR input 1 : logic 0<br>XOR input 2 : variable voltage | 1.17v | 1.21v |
| XOR input 1 : logic 1<br>XOR input 2 : variable voltage | 1.08v | 1.12v |
| Buffer input: variable voltage | 1.48v | 1.80v |

The same experiment is repeated with the resistance connected between the OR gate output and the power supply (5 volts) instead of ground. The resistance is decreased. The recovery mechanism detects the error and disconnects the active module from the system bus. The decreasing resistance pulls up the node it is connected to. The logic 0 voltage level ($V_{OL}$) at that node increases. $V_{IH}$ for the XOR gate being lower than $V_{IH}$ for the buffers, the XOR gate interprets the voltage at the loaded node as a logic 1 before the buffer does. The flip-flop changes state before the buffer produces incorrect data and the recovery is successful. $V_{IH}$ for the buffers and the XOR gate were determined

experimentally using the same setup described in the previous paragraph. The results are shown in Table 1. In summary, if:

$V_{IL(XOR)} > V_{IL(Buffer)}$ and

$V_{IH(XOR)} < V_{IH(Buffer)}$

the XOR chip will detect intermittent failures. Furthermore, the results of the experiments described above show that the stuck-at fault model is not appropriate in the case of intermittent failures. An "intermittent s-a-0" fault at the output of one of the OR gates in the active module should be detected but are not.

## 5.2 Intermittent Failures in the Recovery Mechanism

A variable resistance is connected between the output of the XOR gate and the power supply (5 volts). The resistance is gradually decreased until the recovery mechanism switches off the active module and connects the spare module to the system bus. The recovery is successful and there is no incorrect data on the system bus before or during the changing of state of the J-K flip-flop. It is not necessary to conduct the same experiment with the variable resistance connected to ground instead of the power supply. The output of the XOR gate being 0 in the error-free condition, pulling it down to 0 will not have any effect unless a failure occurs in the active module; in this case, the XOR gate will be unable to produce a 1 at the output, the J-K flip-flop will not change states and the system will fail.

## SUMMARY and CONCLUSIONS

Realistic temporary failures are injected into a simple system that uses dynamic redundancy for fault-tolerance. It is shown that the system does not recover from certain types of temporary failures and that the stuck-at fault model is inappropriate for these temporary failures. Transient failures are induced by decreasing the power supply voltage. Intermittent failures are induced by loading nodes in the system (to ground or Vcc). Decreasing the supply voltage of the active module causes common-mode transient failures that may not detected by the recovery mechanism. Intermittent failures in the active module may or may not be detected depending on the particular electrical characteristics of the components used in the system. Temporary failures in the recovery mechanism are also studied and it is shown that some of them produce a system failure.

Tests are recommended for XOR chips to guarantee detection of temporary failures due to power supply fluctuations and bounds are derived for $V_{IL}$ and $V_{IH}$ of the XOR and the buffers to guarantee detection of intermittent failures.

On-going research shows that the same system built with CMOS catalog parts exhibits similar behavior in the presence of temporary failures. More research need to be done to evaluate of efficiency of other implementations of the recovery mechanism as well as other fault-tolerant schemes.

## ACKNOWLEDGMENTS

This work was supported in part by International Business Machines Corporation (IBM) under a contract with Palo Alto Research Associates (PARA), in part by the Egyptian Government, in part by the "Fundacao de Amparo a Pesquisa do Estado de Sao Paulo" (FAPESP, Brazil) and in part by the Innovative Science and Technology Office of the Stategic Defense Initiative Organization administered through the Office of Naval Research under Contract No. N00014-85-K-0600.

Thanks are due to Lockheed Missiles & Space Company for providing the logic analyzer used in the experiments and to Henk Goosen, David McCluskey and Dr. Takashi Nanya for their comments and suggestions.

## REFERENCES

[Côrtes 86a] M.L. Côrtes, E.J. McCluskey, K.D. Wagner and D.J. Lu, "Properties of Transient Errors Due to Power Supply Disturbances", **Proc. Intern. Symposium on Circuits and Systems - ISCAS 86**, San Jose, California, 1986, pp. 1046-1049.

[Côrtes 86b] M.L. Côrtes and E.J. McCluskey, "An Experiment on Intermittent-Failure Mechanisms," **Proc. Intern. Testing Conference - ITC 86**, Washington D.C., 1986, pp. 435-442.

[Côrtes 87] M.L. Côrtes, "Temporary Failures in Digital Circuits: Experimental Results and Fault Modeling," Ph.D. Dissertation, **Center for Reliable Computing**, Stanford University, Stanford, California 94305.

[Crouzet 82] Y. Crouzet and B. Decouty, "Measurement of Fault Detection Mechanisms," **Proc. FTCS-12**, Santa Monica, California, 1982, pp. 373-376.

[Decouty 80] B. Decouty, G. Michel and C. Wagner, "An Evaluation Tool of Fault Detection Mechanisms Efficiency," **Proc. FTCS-10**, Kyoto, Japan, 1980, pp. 225-227.

[Iyer 82] R.K. Iyer and D.J. Rossetti, "A Statistical Load Dependency of CPU Errors at SLAC", **Proc. FTCS-12**, Santa Monica, California, 1982.

[Lala 85] P.K. Lala, "**Fault Tolerant and Fault Testable Hardware Design**," Prentice Hall, Englewood Cliffs, New Jersey, 1985.

[Losq 75] J. Losq, "Influence of Fault Detection and Switching Mechanisms on the Reliability of Stand-by Systems," **Fault-Tolerant Computing Symposium - FTCS 5**, Paris, France, 1975, pp. 81-86.

[McCluskey 86] E.J. McCluskey, "**Logic Design Principles with Emphasis on Testable Semicustom Circuits**," Prentice Hall, Englewood Cliffs, New Jersey, 1986.

[Schuette 86] M.A. Schuette, J.P. Shen, D.P. Siewiorek and Y.X. Zhu, "Experimental Evaluation of Two Concurrent Error Detection Schemes," **Proc. FTCS-16**, Vienna, Austria, 1986.

[Siewiorek 82] D.P. Siewiorek and R.S. Swarz, "**The Theory and Practice of Reliable System Design**," Digital Press, Bedford, Massachusetts, 1982.

END

DATE

FILMED

DEC.

1987